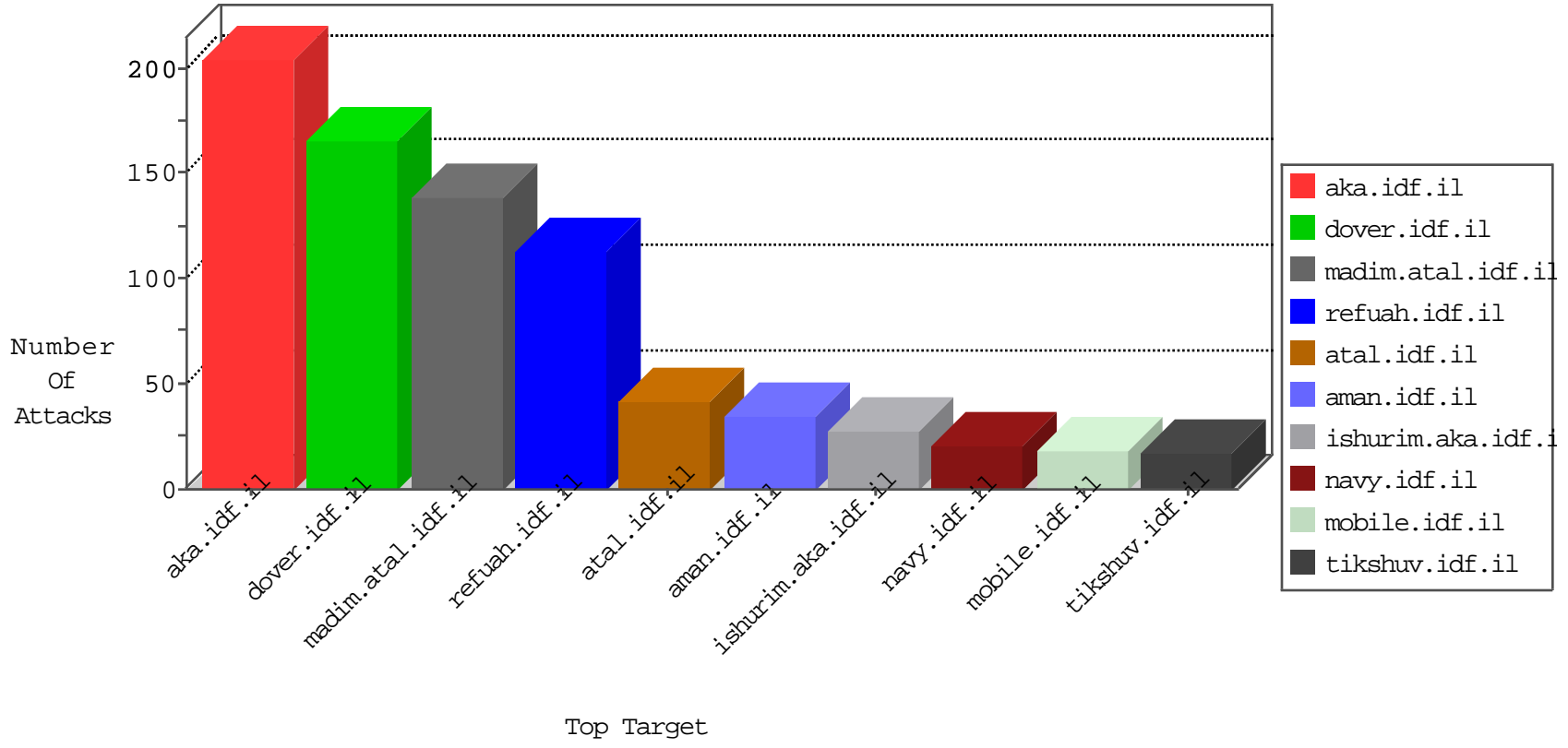


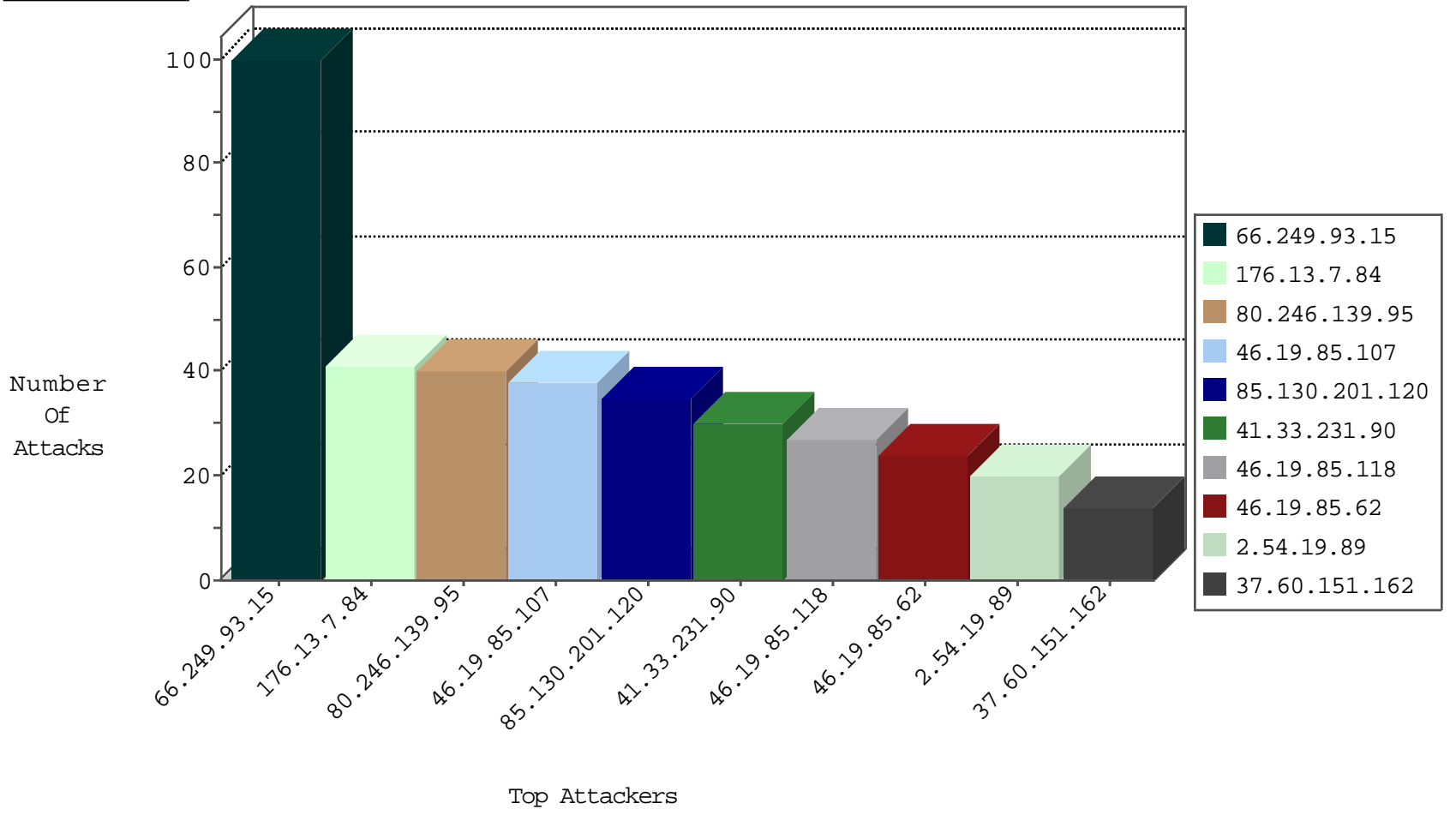
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.171.153	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.65.49.86	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
109.65.49.86	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.103.252.5		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
198.23.190.39	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
109.65.49.86	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.49.86	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
131.253.25.190	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.54.189.237	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.149.232	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.162.167	United Kingdom	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
40.77.167.31	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.3	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.64	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.79	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.15	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	100
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
89.138.105.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.126.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.146.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.27.105.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.199.1	147.237.77.74	Israel	law.idf.il	GPL SCAN myscan	1
2.54.28.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.186.19.37	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.67.249.243	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.11	147.237.76.42	Romania	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
84.228.253.13	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.133.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.1.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.199.1	147.237.77.74	Israel	law.idf.il	INDICATOR-SCAN myscan	1
31.168.198.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.156.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.61.228.113	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
95.67.249.243	147.237.77.74	Russian Federation	law.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.118	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
46.19.85.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
79.183.27.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.64.144.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.60.151.162	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.130.179.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.179.1.218	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
89.138.70.194	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
85.130.201.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.19.89	Israel	147.237.72.156	aman.idf.il	SYN Attack		reject	6
85.130.201.120	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.125.150.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.13.55	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.236.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
85.130.201.120	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.201.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.201.120	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.46	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
66.249.93.248	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
85.130.201.120	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
80.178.157.52	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
176.13.16.32	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
66.249.93.58	Israel	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
84.95.84.77	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.19.89	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
84.108.240.185	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.58.130	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.60.151.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.246.137.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.19.89	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.16.32	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.19.89	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
132.74.44.146	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.168.201.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.189	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.179.9.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.130.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.27.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.133.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.58	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
109.65.200.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.7.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
80.246.139.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
109.253.199.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.32.179.77	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	4
46.19.86.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
134.249.54.139	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi/	Block	3
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.115.64.250	Block	3
46.19.85.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.248.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/a/qaqa/aq/ /q	Block	2
2.54.147.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.250.149.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.238.173.67	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
109.253.199.248	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
85.93.91.84	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
66.249.64.58	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/109545.pdf	Block	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
176.13.11.75	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.148.148	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
80.246.130.208	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
109.253.211.29	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
86.138.172.206	United Kingdom	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
217.69.133.232	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
40.77.167.36	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
46.120.142.4	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
208.80.155.217	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.80.155.217	Block	1
117.253.215.89	India	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
88.198.44.2	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum/templates/http://www.aka.idf.il/sip_storage/files/6/66556.pdf	Block	1
217.139.35.166	Egypt	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
40.77.167.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17968-he/dover.aspx<span style='font-family:tahoma	Block	1
104.131.147.112	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/giyus/qanda/default.asp	None	1
61.131.126.74	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/editor/assetmanager/assetmanager.asp	Block	1
208.80.155.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
5.39.222.159	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/rom-0	Block	1
89.138.70.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
220.181.132.216	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
77.125.97.67	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
81.218.89.58	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
66.249.64.48	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
212.179.1.218	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
37.26.146.152	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
93.113.125.11	Romania	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	1
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/klali.aspx	Block	1